40

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/779,440	02/09/2001	Kentaro Shiomi	60188-031	6677

7590 02/24/2005

MCDERMOTT WILL & EMERY
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/779,440	SHIOMI ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) 8-23 is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1 and 2 is/are rejected.

7)☐ Claim(s) 3-7 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 18 July 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4/04, 7/01
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been examined. A reply to the restriction notice mailed on August 30, 2004 was received on September 30, 2004.

Election/Restrictions

2. Applicant's election without traverse of Group I: claims 1-7, drawn to a method for designing an LSI using a conversion step to produce an encrypted circuit, classified in class 713, subclass 189 in the reply filed on September 30, 2004 is acknowledged. Claims 8-23 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for the steps listed in the instant claim 2 (see Specification, pgs 10-13), does not reasonably provide enablement for step of encrypting provided circuit design data, which covers any encryption of circuit design data. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make or use the invention commensurate in

scope with these claims. The invention of claim 1 is broader in scope then the enabling portion of the specification.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 1 is rejected under 35 U.S.C. 101 as not being tangibly embodied. The claimed invention as a whole must accomplish a practical application. That is, it must produce a "useful, concrete and tangible result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. The step of "encrypting provided circuit design data" is not defined as requiring the use of hardware to accomplish the step; since the system is not directed to a specific hardware element, the claims are non-statutory.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leydier U.S. Patent No. 6,490,646 (hereinafter Leydier).

10. Leydier discloses a method for designing circuits, comprising the step of encrypting provided circuit design data. See Leydier, Figure 3. Leydier does not expressly disclose designing for LSI circuits. However, Leydier does teach encrypting the circuit design within smart cards, wherein the encrypted circuit design secures the values of secret keys. See Leydier, col. 1:10-14 and 41-47; moreover, LSIs are conventionally used within modules of reduced size such as handheld calculators and IC cards. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method to design a secure LSI since LSIs are used in smart card design and design analysis enables attackers to procure sensitive information during cryptographic computation as known to one of ordinary skill in the art and as taught by Leydier, ibid.

11. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al. U.S. Patent No. 6,088,452 (hereinafter Johnson).

12. Johnson discloses a method for designing circuits, comprising the step of encrypting provided circuit design data. See Johnson, col. 11:35-12:20. Johnson does not expressly disclose designing for LSI circuits. However, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method to securely design an LSI since LSIs are incorporated in portable calculating devices, which can be easily isolated to copy the circuit design as known to one of ordinary skill in the art and as taught by Johnson, ibid.

13. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leydier in view of Johnson.

14. As per claim 2, the rejection of claim 1 over Leydier is incorporated herein. Further, Leydier discloses the encrypting step includes the step of conducting circuit conversion to produce an encrypted circuit, the circuit conversion being conducted using an entire circuit represented by the circuit design data or a part of the circuit as an original circuit, the circuit conversion step includes the steps of providing at least one dummy circuit in parallel with the original circuit, the dummy circuit having a same number of inputs and a same number of outputs as those of the original circuit. See

Leydier, Figure 3; A0' ... A15' and D0' ... D7' is dummy circuit parallel with A0 ... A15 and D0 ... D7.

15. Leydier does not disclose permutating the respective outputs of the original circuit and the dummy circuit nor providing a selector responsive to a selection signal for selecting a number of signals corresponding to the number of outputs of the original circuit from an output of the permutation circuit so as to produce the encrypted circuit, wherein the selection signal is used as a key signal, and such a value of the key signal that the output of the original circuit matches an output of the selector is used as a key of the encrypted circuit. Johnson teaches an encoding technique for hardware including a permutation means for permutating the respective outputs of the original circuit and the dummy circuit, and providing a selector responsive to a selection signal for selecting a number of signals corresponding to the number of outputs of the original circuit from an output of the permutation circuit so as to produce the encrypted circuit, wherein the selection signal is used as a key signal, and such a value of the key signal that the output of the original circuit matches an output of the selector is used as a key of the encrypted circuit. See Johnson, Figure 7; 9:47-11:9; 12:1-20; the selector responsive to a selection signal, which is used as a key signal is covered by the intertwining functions A and B in Figure 7; the type of intertwining function used is based on the selection signal, col. 12:17-18. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to apply the obfuscating technique to the method of Leydier. Motivation to combine protects the intelligence of the design of the circuit from

being discovered. See Johnson, 1:5-12. The aforementioned cover the limitations of claim 2.

Allowable Subject Matter

16. Claims 3-7 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Pechar U.S. Patent No. 4,583,011 discloses a circuit to prevent copying of a MOS circuit.

Johnson et al. U.S. Patent No. 5,748,741 discloses encoding technique for hardware.

Takanki U.S. Patent No. 6,137,318 discloses a circuit having a dummy MOS transistor.

Collberg et al. WO 9901815 discloses obfuscation techniques for enhancing software security.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
February 16, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100